

North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

*Indicated a mandatory field

*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

AKERMAN LLP

Entity Type: GENERAL BUSINESS
Address: 495 NORTH KELLER ROAD
Apt/Suite/Building: SUITE 300
City: MAITLAND
State: FL
Zip Code: 32751
Telephone: (407) 254-3594
Fax:
Email: PATTI.GREBER@AKERMAN.COM

*Date Security breach Reporting Form Submitted: 05/13/2015
*Date the Security Breach was discovered: 04/07/2015
Breach Type: HACKERS/ UNAUTHORIZED ACCESS
*Estimated number of affected individuals: 4
*Estimated number of NC residents affected: 1

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))
PREMERA BLUE CROSS

Describe the circumstances surrounding the Security Breach: ON JANUARY 29, 2015, PREMERA BLUE CROSS ("PREMERA"), DETERMINED THAT IT WAS THE VICTIM OF WHAT IT DESCRIBES AS A SOPHISTICATED CYBER-ATTACK. ON MARCH 17, 2015, PREMERA PUBLICLY DISCLOSED THE BREACH. PREMERA REPORTS THAT IT DELAYED ANNOUNCING THE ATTACK BASED ON ADVICE IT RECEIVED TO FIRST FOCUS ON BLOCKING THE ATTACK AND CLEANSING ITS IT SYSTEMS TO PREVENT FURTHER MALICIOUS ACTIVITY BY THE CYBER-ATTACKERS. SHORTLY AFTER PREMERA ANNOUNCED THE BREACH, BCBSF, THE ADMINISTRATOR FOR THE SELF-INSURED EMPLOYEE HEALTH PLAN MAINTAINED BY AKERMAN LLP, NOTIFIED AKERMAN OF THE BREACH, BUT ADVISED THAT IT WAS UNKNOWN IF ANY AKERMAN PLAN PARTICIPANTS WERE AFFECTED. ON APRIL 7, 2015, BCBSF CONFIRMED THAT SOME AKERMAN PLAN PARTICIPANTS WERE AFFECTED BY THE ANTHEM BREACH.

Information Type: ACCOUNT #
MEDICAL INFORMATION
SSN

*Regarding information breached, if electronic, was the information protected in some manner:

NO

If YES, please describe the security measures protecting the information:

*Describe any measures taken to prevent a similar Security Breach from occurring in the future:

ACCORDING TO PREMIER, IT HAS CLEANED ITS INFORMATION TECHNOLOGY SYSTEMS. IT HAS ALSO ENGAGED A LEADING CYBERSECURITY FIRM TO STRENGTHEN THE SECURITY OF ITS SYSTEMS.

*Date affected NC residents were/will be notified:

05/06/2015

Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):

NOT APPLICABLE

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. 75-65 (e)):

WRITTEN NOTICE

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained

- Notification to major statewide media

Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Contact Information SAME AS ABOVE
Affiliation with entity
experiencing breach:

Organization Name:

Prefix:

*First Name: PATTI

Middle Name:

*Last Name: GREBER

Suffix:

Title:

Address:

Apt/Suite/building:

City:

State:

Zip Code:

*Telephone: (407) 254-3594

Fax:

Email: PATTI.GREBER@AKERMAN.COM

Patti L. Greber
Director of Human Resources

Akerman LLP
National Administrative Group
495 North Keller Road, Suite 300
Maitland, FL 32751
Tel: 407.423.4000
Fax: 407.843.6610

Dir: 407.254.3594
patti.greber@akerman.com

May 6, 2015

Re: Impact to You of Recent Premera Breach

Dear:

As you may be aware from recent news reports, in March 2015, a health insurance company in the Pacific Northwest, Premera Blue Cross ("Premera"), disclosed that it had been the victim of a sophisticated cyber-attack. We are writing to inform you that Premera has determined that you are one of the individuals whose personal information was improperly accessed as a result of the cyber-attack.

At the time of the initial news reports of the Premera breach on March 17, 2015, Akerman contacted Blue Cross Blue Shield of Florida (BCBSF) to determine if any Akerman BCBSF participants were affected. BCBSF advised that it was unknown if any Akerman BCBSF participants' information was involved in the data breach. However, on April 7, 2015, BCBSF confirmed that some Akerman BCBSF participants were affected by the breach and provided us with the names of individuals who Premera determined to be affected BCBSF members. Regrettably, your name was included on the list we received.

Premera reported that the cyber-attackers gained unauthorized access to its information technology systems and, as a result, obtained certain personal information of its members. Premera also reported that it discovered the data breach on January 29, 2015, but its investigation showed that the initial attack on its systems occurred on May 5, 2014. According to Premera, the cyber-attackers may have gained access to your information which could include names, birth dates, medical identification numbers, street addresses, email addresses, telephone numbers, social security numbers, and claims information, including clinical data of current and former plan participants. At this point, Premera reports that its investigation has not determined that this improperly accessed information was removed from its information technology system. Premera also reports that it has no evidence to date that the improperly accessed data has been used inappropriately.

As soon as our firm was made aware of the cyber-attack and the potential impact it could have on Akerman BCBSF participants, we immediately began working very closely with BCBSF to monitor the situation in order to provide updates to our employees as soon as information was available. We remain in close communication with BCBSF and will continue to monitor, assess

and report any new findings, as needed.

According to Premera, it has worked closely with one of the world's leading cybersecurity firms to conduct an investigation and to remove the infection created by the attack on its IT systems. Premera says that it delayed announcing the attack based on advice it received to first focus on blocking the attack and cleansing its IT systems before advising the public of the breach in an effort to prevent the cyber-attackers from engaging in additional malicious activity. Premera has also contacted the FBI about the breach and is coordinating with the FBI's investigation into the attack. Premera says that it is taking additional actions to strengthen and enhance the security of its IT systems moving forward.

You may wonder why a breach at Premera affects you, since your plan is administered by BCBSF, not Premera. The impact of this cyber-attack extends beyond Premera's members because Premera maintains personal information on other individuals who may have received health care services covered under the BlueCard program. As you may know, the BlueCard program enables members of one Blue Cross and Blue Shield Plan to obtain coverage for health care services while traveling or living in another Blue Cross and Blue Shield Plan's service area. BCBSF plan participants who received BlueCard-covered health care services that were administered by Premera since 2002 (i.e., had their health insurance claims processed by a Premera-affiliated plan) were potentially impacted by this cyber-attack. Separately, we have also been advised by BCBSF that plan participants who have had medical testing or lab work performed in one state and sent to a facility in another state covered by Premera could also be impacted. For example, you may have had blood drawn in Florida, but the sample happened to have been sent to Washington state for processing. Premera operates affiliated plans in Washington state and Alaska.

As a result of this breach affecting your information, we encourage you to take the following precautionary measures to protect your credit and identity:

Free Credit Monitoring and Repair – Premera is offering to affected or potentially affected individuals a free, two year membership in Experian's® ProtectMyID® Alert to help detect possible misuse of your information and provide you with identity protection services focused on immediate identification and resolution of identity theft. You may enroll in these services or obtain additional information concerning the Premera data breach online at www.premeraupdate.com or by calling Premera at 1-800-768-5817, Monday through Friday, between 5:00 a.m. and 8:00 p.m., Pacific Time (closed on U.S. observed holidays). TTY/TDD users should call 1-877-283-6562.

Free Credit Reports - To find out more about protecting your identity, you can contact the Federal Trade Commission: (1) toll free at 877-438-4338; (2) online at www.consumer.gov/idtheft; or (3) in writing at The Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The Federal Trade Commission has counselors who can tell you how to contact the credit bureaus to get a free credit report or to freeze your credit.

Here is contact information for three major consumer reporting agencies:

Equifax PO BOX 740241 ATLANTA, GA 30374-0241 1-800-525-6285 www.equifax.com	Experian PO BOX 2002 ALLEN, TX 75013 1-888-397-3742 www.experian.com	TransUnion PO BOX 2000 CHESTER, PA 19022 1-800-680-7289 www.transunion.com
--	---	---

North Carolina residents may obtain information from the North Carolina Office of the Attorney General at: <http://www.ncdoj.gov/Crime.aspx>, call 1-919-716-6400, or write to this address:

Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

Prevent Unauthorized Access to Your Accounts - Review your explanation of benefits ("EOB") statements that your health insurer sends to you and monitor free credit reports. Contact your health insurer immediately if you identify medical services on your EOB that you did not receive. Contact your financial institutions to prevent unauthorized access to personal accounts.

Be Aware of Scams – Premera has stated that they are not calling members regarding the cyber-attack and are not asking for credit card information or Social Security numbers over the phone. There are also email scams designed to capture personal information and are designed to look as if they are being sent from Premera. For more information on recognizing scam email, visit the FTC website: <http://www.consumer.ftc.gov/articles/0003-phishing>.

You may have also received similar notification letters from BCBSF and/or Premera. If you have not, you should expect to receive their notification letters in the coming days or weeks. In addition, it is possible that you or a family member could receive a separate notification from Premera (or another Blue Cross entity) because your data from a non-Akerman Blue Cross plan may have been compromised.

We are sorry for the inconvenience the Premera data breach has caused. We at Akerman continue our commitment to safeguarding personal data from unauthorized access.

If you have any questions or concerns, please feel free to contact Blair Stum at (407) 254-3460 or blair.stum@akerman.com, or me at (407) 254-3594 or patti.greber@akerman.com.

Sincerely,

May 6, 2015

Page 4

Patti L. Greber

Director of Human Resources